WHEN THE GOVERNMENT SEIZES
AND SEARCHES YOUR CLIENT'S COMPUTER

By Amy Baron-Evans*

I. Introduction

The Supreme Court has long recognized the "grave danger" to privacy inherent in a search and seizure of a person's papers -- that private documents for which there is no probable cause may be examined in the course of searching for documents described in a warrant. *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). This threat to privacy is heightened in searches of computers because of the broad nature and variety of information stored there. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech 75 (1994). Individuals and businesses use computers to create, store, and communicate every type of information imaginable, from the most public to the most sensitive, including trade secrets, privileged communications, private correspondence, and stray thoughts never intended to see the light of day. Moreover, unlike a paper filing system, any given hard drive is full of information the average user assumes never was or is no longer there -- the content of websites visited, e-mails sent off and forgotten, documents deleted or never deliberately saved.[1] *See* James Fallow, *No Thanks for the Memories*, The Industry Standard, Jan. 15, 2001, at 43; *People v. Gall*, 30 P.3d 145, 181-62 (Colo. 2001) (Martinez, J., dissenting). Furthermore, embedded in any computerized document is information that can appear to be damning evidence that a specific person downloaded, wrote, modified or viewed the document at a certain time, i.e., user Joe Smith wrote the threatening letter on May 4, 2002 between 3:02 and 3:10 P.M., though in fact it may have been Mary Smith who wrote it or the dates and times may have been altered.

Not surprisingly, then, computers are tempting and frequent search targets in criminal investigations of every kind. Fortunately, the technical means exist to search computers for particular information without rummaging through private information not described in a warrant. For example, in a typical white-collar case, relevant files can be isolated and irrelevant ones avoided through keyword searches. In a child pornography case, the government can search for picture files without the need to look at any text file. Thus, just as probable cause to search for a stolen car would not justify the search of a dresser drawer, a search of a computer hard drive can and therefore should be confined to files with attributes tied to probable cause. Without a proper understanding of the technology and its relationship to basic Fourth Amendment principles, however, a number of courts have approved computer searches that in

* Amy Baron-Evans is a partner at Dwyer & Collora, LLP, in Boston, Massachusetts, whose practice consists of defending corporations and individuals in criminal investigations, trials, and appeals.

[1] When a computer file is "deleted," its address is merely changed to "unallocated," but the text remains in "free space" unless it is overwritten, either intentionally or in the course of the computer's normal operation. At the end of every saved file is "slack space," which contains all kinds of unexpected information, including text from other files that were deleted then overwritten by shorter files and text that was never intentionally saved.

the physical world would have been ruled unconstitutional general searches. Educating a judge in this area can be a challenge, but unless you do, the government wins.

II. Know the Law and the Technology

As soon as possible after a subpoena or search warrant is served, hire a forensic computer examiner to educate you about the technology at issue in the case. An expert will be indispensable in framing and justifying discovery requests, reconstructing the government's search, and providing affidavits and testimony in support of a motion to suppress. An expert with substantial experience executing government search warrants can be particularly helpful in recognizing what the government's examiner actually did and why it violated the Fourth Amendment.

For a good start on the caselaw and a look at Department of Justice ("DOJ") policy, the DOJ's Computer Crime and Intellectual Property Section has published guidelines for computer searches in three main volumes, *Federal Guidelines for Searching and Seizing Computers*, 1994 (hereinafter "*Searching and Seizing Computers 1994"), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, January 2001 (hereinafter "*Searching and Seizing Computers 2001*"), and *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002 (hereinafter "*Searching and Seizing Computers 2002*"),[2] and two supplements dated 1997 and 1999. These are surprisingly helpful (though not to be accepted uncritically) and available on the internet at www.usdoj.gov /criminal/ cybercrime. Anyone challenging a search in Massachusetts state court should review a publication of the Attorney General's Office entitled *Internet Crime and Searches of Computers for Clerk-Magistrates*, November 2002, which contains similarly helpful search criteria that may not have been followed in your case. For a generally enlightened approach, *see* Mitchell Kapor & Mike Godwin, *Civil Liberties Implications of Computer Searches and Seizures: Some Proposed Guidelines for Magistrates Who Issue Search Warrants*, and other useful resources at www.sgrm.com.

III. Challenging a Search and Seizure of Computerized Information

The same Fourth Amendment principles that apply to other kinds of searches apply to computer searches. The search and seizure must not only be reasonable, but must be performed pursuant to a warrant, issued on probable cause and particularly describing the place to be searched and the things to be seized. *E.g.*, *Mincey v. Arizona*, 437 U.S. 385, 390 (1987). In a rare case, one of the few exceptions to the warrant requirement may apply. *Id.*

The scope of the search may not exceed the scope of the warrant or the applicable exception to the warrant requirement, or, in any case, the bounds of probable cause. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Walter v. United States*, 447 U.S. 649, 656-57 (1980). The

[2] The 2002 version contains a few new cases and incorporates changes made by the USA Patriot Act to the Electronic Communications Privacy Act, the Wiretap Act and the Pen/Trap Statute. This article primarily cites to the 1994 and 2001 versions, but the 2002 version should be consulted for nuances that may apply in your case.

mere fact that a suspect uses a computer along with an "expert" law enforcement opinion that this type of offender uses computers to store or communicate incriminating information does not amount to probable cause. *See United States v. Weber*, 923 F.2d 1338, 1343-45 (9th Cir. 1991); *State v. Nordlund*, No. 26222-3-II, 2002 WL 2005540, **4-6 (Wash. Ct. App. Aug. 30, 2002).

Just like other searches, the application of Fourth Amendment principles to a computer search depends on the particular facts of the search. What is different about a computer search is that the facts are unfamiliar and difficult to visualize. The challenge is to make the judge understand the technical facts and how the Fourth Amendment applies to them. Analogies to more traditional search settings are helpful, but proceed with caution.

A. The Basic Steps

At the most general level, there are two steps in a search and seizure of computerized information, each of which must comply with the Fourth Amendment: (1) the search for and (possible) seizure of the hardware or other media (e.g., floppy disks) upon which the information described in the warrant is believed to be stored, and (2) the search for and seizure of the particular files or data specified in the warrant. *See United States v. Upham*, 168 F.3d 532, 535-36 (1st Cir.), *cert. denied*, 527 U.S. 1011 (1999).

A computer may be seized because it is itself evidence, fruits or contraband, *e.g.*, one used by a hacker or to create child pornography. However, because there is an expectation of privacy in the contents separate from that in the computer itself, a warrant or an exception to the warrant requirement that authorizes the seizure of a computer will not support a search of its contents. *See United States v. Carey*, 172 F.3d 1268, 1274 (10th Cir.) (consent to seize computer did not permit the officer to open files contained in the computer), *reh'g denied*, 172 F.3d 1268 (10th Cir. 1999); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant for computers and diskettes with no probable cause limitation on which files could be seized was a general warrant); *United States v. O'Razvi*, No. 97 Cr. 1250 (DLC), 1998 WL 405048, *6 (S.D.N.Y. July 17, 1998) (warrant was required to search content of computer disks seized during a search of a briefcase incident to arrest); *United States v. Blas*, No. 90-CR-162, 1990 WL 265179, **19-21 (E.D. Wis. Dec. 4, 1990) (consent to look at electronic storage device does not authorize the activation of the device and search of its contents); *cf. Horton v. California*, 496 U.S. 140, 141 n. 11 (1990) (when a container is seized, contents may not be searched without a warrant). Rather, the warrant and the search itself must "*focus[] on the content of the record*" for which there is probable cause. *Searching and Seizing Computers 1994*, Part IV(H) (emphasis in original).

Conversely, a warrant authorizing a search for certain computer files does not permit the seizure of the computer itself or its entire contents, any more than a warrant authorizing a search of a house for a murder weapon would permit the police to cart off the entire contents of the house.[3] *See Upham*, 168 F.3d at 535-36 & n.1; *Kreman v. United States*, 353 U.S. 346 (1957) ("The

[3] Note that there are earlier cases that missed this point, upholding the seizure of all computers and data pursuant to warrants for the search and seizure of certain records. *See, e.g., United States v. Sissler*, No. 90-CR-12, 1991 WL 239001 (W.D. Mich. Aug. 30, 1991), *aff'd*, 966 F.2d 1455 (6th Cir. 1992), *cert. denied*, 506 U.S. 1079 (1993); *United States v. Musson*, 650 F. Supp. 525, 531-32 (D. Colo. 1986).

seizure of the entire contents of the house and its removal some 200 miles away to the F.B.I. offices for the purpose of examination are beyond the sanction of any of our cases."). The government may be able to obtain authorization to seize a computer for off-site review if it can establish that an on-site search is impractical under the circumstances. *Searching and Seizing Computers 2001*, Parts I(B)(1), II(C)(Step 3) & App. F, Part II(C). This method, however, should be unreasonable where less disruptive means are available, as they often are. *Id*. ("If the hardware is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible."). The government can search the computer on-site and copy the files specified in the warrant at that time, or it can make a "mirror image" of the entire hard drive, then take it off-site, restore it to another hard drive that has been wiped clean, and search for and seize the files and data specified in the warrant. *Searching and Seizing Computers 2001*, Part II(B)(1). The latter is the better forensic practice because searching the original hard drive can compromise the original evidence, and an image is unreadable unless it is restored to another hard drive. Though making a mirror image is a "seizure" only for the limited purpose of getting the information into a searchable form and does not involve any viewing of information, it still should be authorized by the magistrate. *Searching and Seizing Computers 2001*, App. F, Part II(C)(2). If not, it arguably is a seizure in flagrant disregard of the warrant. *See* Part III(B)(1)(b), *infra*.

Be aware that the government may attempt to justify a broad search and seizure by claiming that authorization to make and restore an image of a hard drive permitted it to search for and seize anything and everything on the hard drive. Indeed, courts have been successfully misled by this argument. *See, e.g.*, *United States v. Habershaw*, No. Cr. 01-10195-PBS, 2001 WL 1867803, at *7 (D. Mass. May 13, 2001) (confusing First Circuit's prior holding that a computer may be seized for an off-site search with permission to search and seize entire content). Necessary logistical measures like making a mirror image or removing hardware for off-site review, however, "do[] not expand the theoretical basis of probable cause." *See Searching and Seizing Computers 1994*, Part IV(H). Given the wide variety of information stored on almost any computer or network, it is highly unlikely if not impossible that the government can establish probable cause to believe the entire computer media is filled with evidence of criminal activity.[4]

[4] *See Kow*, 58 F.3d at 427-28 (warrant authorizing seizure of all computer hardware and software was overbroad); *Application of Lafayette Academy, Inc.*, 610 F.2d 1, 3-6 (1st Cir. 1979) (warrant authorizing the seizure of all books, papers and computer tapes, disks, and logs on the premises violated the particularity requirement because the only limitation on the items to be seized was that they be evidence of the violation of specified laws, and consequently also violated the probable cause requirement by authorizing the seizure of items for which there was no probable cause); *United States v. Hunter*, 13 F. Supp.2d 574, 584 (D. Vt. 1998) (section of warrant listing all computers without limitation violated particularity requirement); *cf. United States v. Shilling*, 826 F.2d 1365, 1369 (4th Cir. 1987) ("we cannot condone the wholesale removal of filing cabinets and documents not covered by the warrant"); *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980) (warrant authorizing seizure from an office of all records without limitation was "exactly the kind of investigatory dragnet that the fourth amendment was designed to prevent"); *United States v. Abram*, 830 F. Supp. 551, 554-55 (D. Kan. 1993) (indiscriminate seizure of entire file cabinets exceeded the scope of the warrant and was in flagrant disregard of its terms).

B. The Search of the Contents

In most cases, a criminal defense lawyer's goal will be to suppress information seized from within the computer rather than the computer itself. The law remains fairly undeveloped in this area, but interesting and successful challenges can be mounted.

1. Definitions

What constitutes a search and when a seizure occurs have implications for numerous issues arising in motions to suppress computer searches, including seizures beyond the scope of the warrant, application of the "plain view" doctrine, and whether a search or seizure occurred after the warrant expired.

a. What is a Computer "Search"?

Any technical process used to locate, review, extract, or enhance information is a search when it allows the government to view and seize information that is not exposed to public view, is not already lawfully in the government's possession, and is not in plain view during the course of a lawful search. *Kyllo v. United States*, 533 U.S. 27 (2001) (use of thermal imaging device to detect heat patterns was an intrusion protected by Fourth Amendment); *Arizona v. Hicks*, 480 U.S. 321, 324-35 (1987) (moving stereo equipment to observe serial number was a new "search" separate and apart from the search that was the lawful objective of entering the apartment). According to the DOJ, the use of innovative technology not in general public use to obtain information stored on or transmitted through computers or networks, such as internet surveillance, may amount to a search and therefore require a warrant under *Kyllo*. *See Searching and Seizing Computers 2002*, Part I(B)(5).

b. What is a "Seizure" of Computerized Information?

Like any other type of intangible information, computer files and data should be considered seized for Fourth Amendment purposes when the government copies, extracts, records, saves, writes or prints it from its existing location to another medium. *See Berger v. New York*, 388 U.S. 41, 59-60 (1967) (recording conversations constituted a seizure); *Ayeni v. Mottola*, 35 F.3d 680, 688 (2d Cir. 1994) ("the video and sound recordings were 'seizures' under the Fourth Amendment"); *LeClair v. Hart*, 800 F.2d 692, 694-95 (7th Cir. 1986) (verbatim copying (both tape recorded and handwritten) of financial documents outside the scope of the warrant was an illegal seizure); *Sovereign News Co. v. United States*, 690 F.2d 569, 573-74 (6th Cir. 1982) (taking notes of film and magazine titles constituted a seizure). The seizure should be considered complete at that moment, whether or not it will then be reviewed by a third party for privilege, passed on to the prosecution team, or used by the prosecution team, since Fourth Amendment protection is triggered without regard to the use made of the things seized, *Soldal v. Cook County*, 506 U.S. 56, 67 n.11 (1992); *Warden v. Hayden*, 387 U.S. 294, 301 (1967); *Silverthorne Lumber v. United States*, 251 U.S. 385, 392 (1920), and even if they are not used at all. *See Terry v. Ohio*, 392 U.S. 1, 16 (1968); *Kolendar v. Lawson*, 461 U.S. 352, 362 n. 1 (1983) (Brennan, J., concurring). Indeed, courts routinely refer to government copying of computer data as a "seizure." *See United States v. Longo*, 70 F. Supp. 2d 225, 247 (W.D.N.Y.

1999) (government "seized" a directory listing of the hard drive and computer files which it copied to floppy disks and compact disks); *United States v. Gawrysiak*, 972 F. Supp. 853, 865-66 (D. N.J. 1997) (government "seized" all of defendant's computer files by copying them onto diskettes), *aff'd without opinion*, 178 F.3d 1281 (3d Cir. 1999); *United States v. David*, 756 F. Supp. 1385, 1389, 1392-93 (D.Nev. 1991) (obtaining information from a computer memo book was a seizure).

A seizure, of course, must be pursuant to a warrant or an exception to the warrant requirement and supported by probable cause. A copying process that merely serves a necessary forensic purpose should be described in the search warrant affidavit as such, *see Searching and Seizing Computers 2001*, App. F, Part II(C)(2), but is supported by the same probable cause as that for the hardware itself, *i.e.*, probable cause to believe that the information to be seized is located somewhere on the hard drive or other media. This typically consists of making a mirror image, which is an automated process that gets all the data into a searchable form and does not involve even viewing of data. Or the government may copy a universe of files directly from the computer on-site for a later off-site search without making a mirror image.[5] Be aware, however, that wholesale copying onto CDs or magneto optical disks does not serve a necessary forensic purpose when it is done in addition to making a mirror image, because the image both preserves the original evidence and gets the data into searchable form. Indeed, the DOJ Manuals nowhere mention any forensic need to make a mirror image then copy the same data onto disks. Since CDs are read-only and magneto optical disks can be write-protected, this procedure lends itself to being used for the illegitimate purpose of conducting an overbroad search without leaving a trace.[6]

2. The Search Methodology

A developing challenge to computer searches is the claim that a technical search methodology that minimizes unwarranted intrusions on privacy is required as a constitutional matter. *Cf. Andresen*, 427 U.S. at 482 n.11 ("responsible officials, including judicial officials, must take care to assure that [searches and seizures of a person's papers] are conducted in a

[5] The government copied all of the files from the defendant's computer on-site in *United States v. Gawrysiak*, 972 F. Supp. 853 (D. N.J. 1997). The court found that it did so in good faith, reasoning that the agents' only other option would have been to cart away the hardware, a result that would have been much more intrusive. Id. at 866. The court did not have to reach the question of whether this seizure constituted flagrant disregard of the warrant, which did not authorize the wholesale copying of the files, because the government mooted that claim when it did not read any of the files, did not plan to use any of them at trial, and informed the court it would return them to the defendant. *Id.*

[6] In *United States v. Triumph Capital Group, Inc.*, No. 3:00CR217, 2002 WL 31487754 (D. Conn. Nov. 4, 2002), however, the court deemed wholesale copying onto CDs in addition to making a mirror image and working copies of the image to be "simply preliminary and reasonably necessary steps in the forensic examination." *Id*. at *35. The court credited the agent's testimony that his labeling of the CDs as "seized files" was just a "bad choice of words," and that he made the CDs to serve as a record of the data and files that he had "extracted" from the hard drive and to record his keyword searches. *Id*. This made no sense, however, as it was not explained how an "extraction" was different from either a seizure or a mirror image, and the CDs contained no physical evidence of a keyword search.

manner that minimizes unwarranted intrusions on privacy."); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 463 (5th Cir. 1994) ("The purpose of the minimization requirement [for the interception of electronic communications] is to implement 'the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized.'"). The failure to use such means can support a claim that the search was overbroad or in flagrant disregard of the warrant (requiring suppression of all items seized), and negate government defenses such as good faith and plain view.

The argument follows from the particularity requirement and the overbreadth doctrine. The particularity requirement aims to prevent excessive seizures and exploratory rummaging by requiring that the description of the things to be seized be limited to the scope of probable cause established in the warrant, and that the warrant tell the officers how to separate those items from irrelevant ones, leaving nothing to their discretion. *See Andresen*, 427 U.S. at 480; *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Marron v. United States*, 275 U.S. 192, 296 (1925); *Upham*, 168 F.3d at 535; *Searching and Seizing Computers 2001*, Part II(C)(Step 1).

The overbreadth doctrine, which applies to searches with or without a warrant, requires that the search be limited to the specific things and areas for which there is probable cause. The scope of a lawful search must be limited to the areas in which the object of the search reasonably may be found. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Thus, probable cause to believe that a stolen lawnmower will be found in a garage will not support a search of an upstairs bedroom, nor will a warrant for a stolen refrigerator authorize the opening of desk drawers. *See id*. at 84; *United States v. Ross*, 456 U.S. 798, 824 (1982); *Walter v. United States*, 447 U.S. 649, 657 (1980). "If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more." *Horton v. California*, 496 U.S. 128, 140 (1990).

In other words, every search is subject to inherent area limitations, whether spelled out in a warrant or not. The DOJ acknowledges that the law prefers searches of all things, including computer data, "to be as discrete and specific possible," *Searching and Seizing Computers 1994*, Part IV(G)(3), and advises agents to carefully explain in the affidavit the specific set of techniques they will use to distinguish incriminating documents intermingled with innocuous ones. *Searching and Seizing Computers 2001*, Part II(A), (C)(Step 3) & App. F, Part II(C)(2), (3).

Various technical means are available to enable the government to confine the search to the scope of probable cause, including searching by filename, directory or sub-directory; the name of the sender or recipient of e-mail;[7] specific key words or phrases;[8] particular types of

[7] *See United States v. Maxwell*, 45 M.J. 406, 420 (C.A.A.F. 1996) (search of e-mails associated with names not listed in the warrant enlarged seizure beyond that established by probable cause).

[8] With an automated keyword search, distinctive words, phrases, or combinations of words or phrases, can be used to identify only those files or fragments of deleted files that are specified in the warrant. A keyword search will locate words and phrases in most areas of the hard drive, including active files, free space, slack space and internet cache files. Though it will not pick up keywords in files stored in

files as indicated by filename extensions;[9] and/or file date and time.[10] Depending on the circumstances, the government may be required to confine the search to a specific compartment of the hard drive, for example, the storage area for e-mail.[11] These techniques essentially circumscribe the "areas" where the agent is permitted to search for the items she is authorized to seize.[12] Be aware that this is another area where the judge must be carefully educated lest she be misled. For example, in *United States v. Habershaw*, *supra*, the district court misinterpreted a First Circuit decision approving the government's recovery of deleted files described in a warrant, *see Upham*, 168 F.3d at 537, to mean that the government could use any means to retrieve information described in a warrant, including a sector by sector search of every bit of data on the hard drive. *Habershaw*, at *8. The issue of an overbroad search methodology, however, was not reached by the *Upham* court.

To justify a wide-ranging search (which invariably results in the seizure of evidence "in plain view" that was not described in the warrant), the government can be counted on to make

---

Microsoft Outlook, such as e-mail, the Outlook storage file can be opened and then searched for key words from within Outlook. Even encrypted files can be searched for key words, if they can be decrypted at all.

[9] File name extensions can be used to identify those types of files specified (or not specified) in the warrant, such as .xls for spreadsheets, .jpg for graphics files, .HTML for internet files, or .doc for word processing files created by the user. *See United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) (agent did not exceed scope of warrant when he opened a file containing child pornography because he found it in the course of searching the spreadsheet folder with the expectation that that folder would contain records of drug trafficking); *Carey*, 172 F.3d at 1273 (agent exceeded scope of warrant in opening JPG files expecting that they would contain child pornography rather than material related to drugs).

[10] *E.g.*, *United States v. Ford*, 184 F.3d 566, 576 (6th Cir. 1999) ("Failure to limit broad descriptive categories by relevant dates, when such dates are available to the police, will render a warrant overbroad.").

[11] In *Commonwealth v. Hinds*, 437 Mass. 54 (2002), the defendant gave consent over the telephone to search his computer for electronic mail relating to a homicide investigation of his brother. The agent then searched a regular directory and found filenames indicative of child pornography "in plain view." For the first time on appeal, the defendant argued that he reasonably believed in giving his consent that the agent would only be looking in the file where electronic mail is typically stored. Because the record was silent on how and where electronic mail is stored in general or specifically on the defendant's computer, the court declined to reach the issue. *Id*. at 59-60 & n.2.

[12] *See Searching and Seizing Computers 1994*, Part IV(G)(3); *Carey*, 172 F.3d at 1275-76; *Steve Jackson Games*, 36 F.3d at 463; *United States v. Orefice*, No. 98 CR. 1295 (DLC), 1999 WL 349701, *2 (S.D.N.Y 1999); *Hunter*, 13 F. Supp.2d 574, 584 (D. Vt. 1998); *Gawrysiak*, 972 F. Supp. at 860, 866; *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994); *Commonwealth v. Greineder*, Cr. No. 108588 at 91-93 (Mass. Super. Super. Ct. Oct. 18, 2000) (unpublished); *see also* 2 Wayne R. LaFave, *Search and Seizure* § 4.10 (3d ed. Supp. 2001) (Because "a different kind of selectivity is possible," it "should be followed as to computer files."); *cf. United States v. Tamura*, 684 F.2d 591, 595 (9th Cir. 1992) ("sufficiently specific guidelines for identifying the [paper] documents sought [must be] provided in the search warrant").

the general claim that files can be encrypted or mislabeled, or that "criminals" do not keep records of their criminal transactions in files labeled "crime," a notion that originated in paper search cases. *See, e.g., United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990). This argument has been successful in a number of cases where a technically naïve judge simply takes it for granted that it applies in the case at issue. Fight it with the facts of your case. Though a hacker may be adept (or not) at hiding computerized information, the average user is not that sophisticated. Moreover, it is almost never the case that reading through every file is the way to find hidden information. For example, an encrypted file cannot be read unless it is first identified and then decrypted if possible, neither of which is accomplished by reading through all the files. If files are intentionally mislabeled, a keyword search will produce a hit in most areas of the drive (including active files, free space, slack space and internet cache files), and is more effective and more efficient than reading through all of the files. In any event, according to DOJ policy, if searching agents have reason to believe that a "narrow approach will be technically impossible," for example, because the targeted files may be "written using code words to escape detection" by means of a "key word" or other narrowing search methodology, the agent should inform the magistrate of these issues in the affidavit. *See Searching and Seizing Computers 2001*, Part II(C)(Step 3). If it seeks to justify a broad search after the fact, it must support the need for having done so with facts particular to the case. *See Carey*, 172 F.3d at 1274-75 & n.8 (rejecting government's argument that agent had to open every file because the file names may have been misleading because it was not representative of the facts of the case).

As the DOJ acknowledges, most courts favor a targeted approach because it minimizes the possibility that the government will use a warrant for a narrow list of items to justify a broad search and seizure. *See Searching and Seizing Computers 2001*, Part II(C)(Step 3) (citing *Carey*, 172 F.3d at 1275-76; *United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000); *Gawrysiak*, 972 F. Supp. at 866). *See also Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 463 (5th Cir. 1994); *United States v. Orefice*, No. 98 CR. 1295 (DLC), 1999 WL 349701, *2 (S.D.N.Y 1999); *In re Grand Jury Subpoena Duces Tecum*, 846 F. Supp. at 13; Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. at 108. These courts are correct, since a fundamental purpose of the Fourth Amendment is to prevent broad exploratory searches. In a search for drugs, there generally is no need for a careful search methodology because an incriminating bag of white powder is easily distinguished from innocent, private items in the same area. But in a wiretap case, interception of conversations unrelated to the crime under investigation must be minimized. *Berger v. New York*, 388 U.S. 41, 59-60 (1967). Likewise in a search of papers, judicial officials and government agents "must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions on privacy." *See Andresen*, 427 U.S. at 482 n.11; *see also Tamura*, 694 F.2d at 595-96 & n.3 ("sufficiently specific guidelines for identifying the documents sought [must be] provided in the search warrant and . . . followed by the officers conducting the search"). Because a "different kind of selectivity is possible" as to computer files, it "should be followed." *See* 2 Wayne R. LaFave, Search and Seizure § 4.10 (3d ed. Supp. 2001).

In response, the government is likely to analogize a computer search to a search of documents in a file cabinet, claiming that "computer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy." *United States v. Hunter*, 13 F. Supp.2d 574, 584 (D. Vt. 1998). In fact, a search for

data in a computer is like a search for documents in a file cabinet only insofar as both contain records for which there is probable cause intermingled with irrelevant ones. There the similarity ends, because a search for information on a computer can be accomplished through keyword searches and other technological means without unnecessary review of material for which there is no probable cause. *See Carey*, 172 F.3d at 1274-75 (finding the file cabinet analogy inadequate in a case where the searching agent relied on a warrant for documentary materials to view files containing images of pornography, since methods such as key word searches could have been used to avoid searching files of a type not identified in the warrant). In *Hunter* itself, the court held that a portion of the warrant for computers and related equipment was insufficiently particular in that it did not contain or reference search instructions designed to minimize intrusions on irrelevant and privileged material. 13 F. Supp.2d at 584-85. Thus, the statement in *Hunter* about the constitutionality of scanning all documents in a computer was simply dicta contrary to its actual holding.

Nonetheless, *Hunter*'s dicta and the analogy to papers in a file cabinet are commonly promoted by the government and sometimes accepted by courts. This can create huge "plain view" windfalls for the government. For example, in *United States v. Gray*, 78 F. Supp.2d 524 (E.D. Va. 1999), the court found that an FBI Computer Analysis and Response Team agent had acted lawfully in opening and viewing every file because it was purportedly necessary to determine whether or not each one was within the scope of the warrant, characterizing the procedure as proper "routine" practice for the FBI. *Id.* at 529 n.8, 531 n.11. This broad permission to search included graphics files (where the agent opened files depicting child pornography in "plain view"), even though the warrant was only for text files, because the agent did not know how to use his own program to determine whether a file was of pictures or text without viewing it, and it would be unreasonable to expect the FBI to keep up with advanced computer searching techniques. *Id*. at 527 n.4, 529 n.8.

A more apt analogy than a file cabinet is that individual files in a computer are like individual file folders containing paper documents in that the contents are not exposed to public view and are therefore subject to a reasonable expectation of privacy. *See United States v. Knoll*, 16 F.3d 1313, 1320-21 (2d Cir.), *cert. denied, Gleave v. United States*, 513 U.S. 1015 (1994). As a result, the government must have probable cause to open and view a certain computer file, *see United States v. Barth*, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998), and probable cause will depend on the nature and attributes of the particular file. *Cf. Walter*, 447 U.S. at 657 ("a warrant to search for a stolen refrigerator would not authorize the opening of desk drawers."). For example, there may be probable cause to search for a particular contract between two companies, but no probable cause to open files in which a keyword search distinctive to the contract did not produce a "hit." In a child pornography case, there may be probable cause to search for graphics files, but not in a business fraud case. Or there may be probable cause to search for certain files created by the user, but not cache files or swap files, which the computer itself downloads and maintains. Distinctions like these should dictate the search methodology, the scope of the search, and the limits of exceptions to the warrant requirement. *See United States v. Maxwell*, 45 M.J. 406, 421-23 (C.A.A.F. 1996) (opening and viewing an e-mail not listed in the warrant exceeded the scope of the warrant, was not in good faith, was not in plain view, would not have been inevitably discovered, and its fruits were inadmissible).

This is the approach taken by the Tenth Circuit. *See Carey*, 172 F.3d at 1274-75 (consent to seize computer did not permit opening of individual files in the computer, which required a warrant specifying the type of files sought); *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) ("Officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant."). The Fifth Circuit, however, views the container to which the expectation of privacy attaches as the entire hardware and not the individual files. *See United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001) (private search of some files on a computer disk permitted law enforcement to open additional files on the same disk); *United States v. Slanina*, 283 F.3d 670, 680 (5th Cir. 2002) (once warrantless search of a portion of a computer and zip disk had been justified as a government workplace search, comprehensive search of entire content of computer by FBI was permissible). The Tenth Circuit's approach is the correct one because it accounts for the key differences between computer media and containers in the physical world. *Carey*, 172 F.3d at 1275 ("[r]elying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."). That is, because even a desktop computer "can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer," and officers therefore "cannot simply conduct a sweeping, comprehensive search of a computer's hard drive." *Walser*, 275 F.3d at 986.

3. Flagrant Disregard of the Warrant

To obtain blanket suppression of all of the evidence seized, whether or not within the scope of the warrant, the defense must establish that the search was conducted in "flagrant disregard" of the terms of the warrant. The rationale for this remedy is to make the government pay a price for what amounts to a general search. *See United States v. Liu*, 239 F.3d 138, 140-41 (2d Cir. 2000). In order to make the necessary showing, you will need all of the evidence seized by the computer specialist (not just the evidence the prosecution intends to use) and complete documentation of the manner of the search, or a lack thereof.

An essential requirement for blanket suppression is that a substantial quantity of the material seized is outside the scope of the warrant, *see, e.g., United States v. Liu*, 239 F.3d 138, 140 (2d Cir. 2000); *United States v. Squillacote*, 221 F.3d 542, 556-57 (4th Cir. 2000); *United States v. Heldt*, 668 F.2d 1238, 1262 (D.C. Cir. 1981), whether it relates to the crime under investigation, some other crime, or is completely innocuous. *See United States v. Foster*, 100 F.3d 846 (10th Cir. 1996); *United States v. Medlin*, 842 F.2d 1194 (10th Cir. 1988); *United States v. Dzialak*, 441 F.2d 212, 215 (2d Cir. 1971). The defense may have to show that the search resembled a general search in some additional way, such as "indiscriminate rummaging," *Liu*, 239 F.3d at 140-41, or a failure to adhere to area limitations.[13] *United States v. King*, 227 F.3d

[13] To establish flagrant disregard of a warrant in the Second Circuit, the defense must show that the agent "effect[ed] a widespread seizure of items that were not within the scope of the warrant," that the search "*actually resemble[d]* a general search," and, furthermore, that the agent did "not act in good faith." *See United States v. Liu*, 239 F.3d 138, 140-41 (2d Cir. 2000) (emphasis in original). The lack of good faith requirement is distinctive to the Second Circuit. In *United States v. Triumph Capital Group, Inc.*, No. 3:00CR217, 2002 WL 31487754 (D. Conn. Nov. 4, 2002), the defendants claimed that the agent

732, 751 (6th Cir. 2000); *Heldt*, 668 F.2d at 1262. Thus, a failure to follow a narrow and systematic search methodology, whether or not such a methodology was attached to the warrant, often is important in seeking blanket suppression of the fruits of a computer search. *See Gawrysiak*, 972 F. Supp. at 864-65 (measures taken to narrow the search were a factor in finding no flagrant disregard).

An interesting approach for blanket suppression of evidence seized in a computer search would be to show that the lawful and unlawful parts of the search are inextricably intertwined and cannot be unraveled after the fact. *See United States v. Young*, 877 F.2d 1099, 1105 (1st Cir. 1989); *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1979); *United States v. Chang*, 838 F. Supp. 695, 702 n.13, 704 (D.P.R. 1993).

4. Continuing and Multiple Searches

Fed. R. Crim. P. 41 requires a search to be conducted within ten days of issuance of the warrant, and the return to be filed promptly. For a search to be reasonable under the Fourth Amendment, a "warrant may be executed only once," and "once the authorized search has been completed the police must promptly depart the premises." *See* 2 Wayne R. LaFave, Search and Seizure 679 (1996); *see also Sgro v. United States*, 287 U.S. 206, 210 (1932); *United States v. George*, 975 F.2d 72, 80 (2d Cir. 1992); *United States v. Gagnon*, 635 F.2d 766, 769 (10th Cir. 1980). The filing of a search warrant return by definition signifies the end of a search because the inventory of the items seized enables the magistrate to assure herself of the legality of the search. *See* Fed. R. Crim. P. 41(d); *United States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir. 1982). Thus, once the return is filed, a return to the scene to conduct a further search is a warrantless search. *See United States v. Hall*, 678 F. Supp. 1172, 1173-74 (W.D. Pa. 1988). A failure to comply with the warrant's time limits supports a claim that the government flagrantly

---

flagrantly disregarded the warrant by, *inter alia*, seizing a large quantity of information outside the warrant's scope, conducting the search in a manner broader than that described in the search warrant affidavit, searching beyond the time limits required by Fed. R. Crim. P. 41 and the date stated in the return, and failing to keep records of the search. The district court held that even the improper wholesale seizure of information beyond the scope of the warrant did not merit blanket suppression because the search did not actually resemble a general search and was conducted in good faith. The court reached this conclusion by analyzing each Fourth Amendment violation the defense raised according to a reasonableness standard and crediting each of the agent's explanations for his actions as reasonable and therefore in good faith. The opinion fails to explain why it jumped directly to a reasonableness inquiry without first deciding whether the agent violated the Fourth Amendment (*e.g.*, by exceeding the scope of the warrant and the bounds of probable cause), but it appears this was the court's way of responding to the flagrant disregard standard in the Second Circuit, *i.e.*, if the agent had a reasonable explanation then there could be no bad faith and therefore no flagrant disregard. The opinion, however, often seems to apply a subjective good faith standard (when the correct standard is objective good faith) and does not grapple with contrary evidence tending to show objective unreasonableness. By doing so, it creates a picture of a careful search, which may be useful in other cases challenging searches that deviate from the search as described. Otherwise, the opinion is not widely applicable, as it is very case specific, deals only with the flagrant disregard standard in the Second Circuit, applies a seemingly incorrect subjective good faith standard, and has not yet been appealed.

disregarded the warrant, requiring blanket suppression, or at least suppression of evidence seized after the authority to search expired.

The government is likely to take the position that it is entitled to search an image of a hard drive as many times and for as long as it wishes, even after the return is filed. The DOJ maintains that Rule 41(c)(1) "does not apply to the forensic analysis of evidence that has already been seized; however, even if such analysis involves a Fourth Amendment 'search' in some cases, it plainly does not occur in the 'place … named' in the warrant." *Searching and Seizing Computers 2001*, Part II(D)(2). All this should mean, however, is that the government can analyze data that it had already seized before its authority to search expired, much like it can perform ballistics test on a seized bullet without regard to time limitations.

Whether that analogy applies to the search at issue depends on what the warrant authorized the government to seize and what it seized before and after the deadline. For example, if the warrant authorized the seizure of a list of files, and the agent copied all or some of them from an image of the original medium to another medium (e.g., a disk) after the warrant expired, he was seizing new evidence, not merely analyzing evidence already seized. If the agent returned to a mirror image, even to analyze data he had already copied to another medium, this arguably is no different than returning to a house after a warrant expires to conduct further tests on fingerprints or bloodstains. The government may defend such a search by arguing that once the mirror image was made, the search and seizure was complete, and any activity thereafter was just a "forensic analysis." This holds water only if the government obtained a warrant to seize the entire content of the hard drive. Unless it established probable cause for an "all records" search, however, that warrant would be invalid. *See In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 855-57 (9th Cir. 1997) (warrant authorizing seizure of all computers was not justified by probable cause); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant for computers and diskettes with no probable cause limitation on which files could be seized was a general warrant*); In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. at 12-14 (subpoena for all computers and computer data was overbroad).

If the government needs to search for new information after the required time limitations, it must seek permission to do so.[14] While it is true that probable cause is unlikely to dissipate in computer data already in the government's possession, limits on the duration of a search also serve the purpose of ensuring adequate judicial supervision of the reasonableness and scope of the search. *Berger*, 388 U.S. at 60; *United States v. Bedford*, 519 F.2d 650, 655 (3d Cir. 1975), *cert. denied*, 424 U.S. 917 (1976). In *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), in which agents took thousands of pages of documents, the court held that "[t]he essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate," and that the government's retention of all the documents for six months may have been "convenient" but was "an unreasonable and therefore unconstitutional manner of executing the warrant." *Id*. at 596, 597 (emphasis supplied). In *Commonwealth v. Ellis*, 10 Mass. L. Rptr.

[14] *See* Sample Search Warrant in *Internet Crime and* Searches *of Computers for Clerk-Magistrates*, November 2002, published by the Massachusetts Attorney General's Office (requesting no more than 60 days beyond the date of the warrant).

429, 1999 WL 815818 (Mass. Super. Ct. Aug. 27, 1999), the court ruled that a two-year computer search was permissible because it was impractical in that case, which involved a search of thousands of client files in several law offices in an investigation of workers compensation fraud, to expect the agent to complete it sooner. Id. at *8-9. More importantly, the state apprised the court and the defendants throughout the two-year period that the search was ongoing. Where the government continues to search without the court's knowledge or permission, suppression is warranted. *See United States v. Brunette*, 76 F. Supp.2d 30, 42 (D. Me. 1999), *aff'd.*, 256 F.3d 14 (1st Cir. 2001).

Note that this is an area where exactly what the government computer specialist did and when is extremely important, and highlights both the need for accurate records to be kept so that the search can be reconstructed, and the need for a skilled defense expert to reconstruct the search (based on clues such as date stamps) to test the government's representations.

5. Privileged Materials

If the computer is likely to contain privileged communications to or from an attorney, steps to ensure that no member of the prosecution team comes in contact with such communications must be described in the warrant, approved by the magistrate, and followed. *See Hunter*, 13 F. Supp.2d at 579; *Gawrysiak*, 972 F. Supp. 864; *Searching and Seizing Computers 2001*, Part II(B)(7)(b). At minimum, potentially privileged materials should be reviewed by a neutral and independent third party. This can be done in several ways, including by a magistrate judge, a special master, or a so-called "taint team" composed of government lawyers and agents.

"Taint teams" are disfavored because the privilege is invaded when *any* third party reviews privileged communications, the risk of leaks to the "prosecution team" is unacceptably high, and placing such sensitive decisions in the hands of the government in a criminal case at least appears to be unfair. *See United States v. Lin Lyn Trading, Ltd.*, 149 F.3d 1112 (10th Cir. 1998); *Hunter*, 13 F. Supp.2d at 583 n.2; *United States v. Neill*, 952 F. Supp. 834, 840-41 & n. 14 (D.D.C. 1997); *Black v. United States*, 172 F.R.D. 511, 516 (S.D. Fla. 1997); *United States v. Stanfa*, Cr. No. 94-127-1, 1996 U.S. Dist. LEXIS 10314 at *36 (E.D. Pa. July 17, 1996); *In re Search Warrant for Law Offices*, 153 F.R.D. 55 (S.D.N.Y. 1994); U.S. Attorney's Manual § 9-13.420.

When a government "taint team" includes agents "not bound by the ethical considerations which affect a lawyer," the risk of improper disclosure is heightened. *In re Search Warrant for Law Offices*, 153 F.R.D. at 59. The DOJ recommends a "neutral" technical expert to assist the taint team. *Searching and Seizing Computers 2001*, Part II(B)(7)(b). As a practical matter, however, the computer specialist who performs the search functions as a member of both the "taint team" and the "prosecution team" because he must know about the case in order to perform the search, and in fact usually is in regular communication with and taking direction from the prosecution team.

Some courts begin with a presumption that any materials reviewed by a government "taint team" have been disclosed to the "prosecution team," and require the government to prove

the contrary and that the defendant was not prejudiced, before any evidence reviewed by a "taint team" is admissible. *Hunter*, 13 F. Supp.2d at 583; *Neill*, 952 F. Supp. at 841. In one case in which the prosecution team used privileged information in its investigation leading to an indictment, the government was required to begin a new investigation with the prosecutors and agents who were exposed to the privileged material disqualified, if it wished to proceed. *Lin Lyn Trading, Ltd*., 149 F.3d at 1118.

Though the caselaw recognizes the unfairness and unworkability of government taint teams, magistrates regularly approve them in the *ex parte* application for the warrant. The typical procedure is to have a government computer specialist conduct the search then hand the seized materials over to a prosecutor (not involved in the investigation but usually in the same office as the prosecutor handling the case), who then reviews them for privilege, passes on to the prosecution team those materials that she deems not to be privileged, and submits materials that may or may not be privileged to a magistrate judge for decision.

You should move for an alternative procedure as soon as you are aware that a warrant has issued. You might ask for review by a judicial officer, *Black*, 172 F.R.D. at 516-17, or a special master, *Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995), but in order to shield privileged material from *any* government agent, including the computer specialist, that person would have to review all of the files and fragments of files on the hard drive for privilege before turning it over to the computer specialist to perform the actual search.

A better option in a computer search is to have the defense team, with the aid of its own expert, screen all of the data the government computer specialist wishes to search before he searches it, and to have a judicial officer make the final determination as to anything in dispute. Support for such a procedure can be found in cases recognizing the advisability of permitting the defendant and his counsel to be present when a search of papers may encroach upon privileged information. *See Andresen*, 427 U.S. at 466; *National City Trading Corp. v. United States*, 635 F.2d 1020, 1026 (2d Cir. 1980); *Gawrysiak*, 972 F. Supp. at 859.

IV. Challenging Subpoenas

The government may attempt to avoid the probable cause and particularity requirements by subpoenaing a computer or computer disks. The overbreadth doctrine, however, applies to subpoenas under either a Fourth Amendment or Due Process analysis. In *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11 (S.D.N.Y. 1994), the court held that a subpoena for a central processing unit, hard drive, and all computer-accessible data was unconstitutionally overbroad since the hardware contained documents having nothing to do with the grand jury investigation, reasoning that "the expanded investigation does not justify a subpoena which encompasses documents completely irrelevant to its scope, particularly because the government has acknowledged that relevant documents can be isolated through key-word searching." Id. at 12-13. If the government subpoenas a computer, use a motion to quash or narrow the subpoena to seek court-ordered limits on the items seized and a search methodology designed to avoid irrelevant items.

The government may issue a forthwith subpoena for a computer if there are exigent circumstances, *e.g.*, to prevent the destruction of evidence. Since this can effectively deprive the recipient of the ability to move to quash, a forthwith subpoena amounts to a warrantless seizure in violation of the Fourth Amendment if it was issued without sufficiently exigent circumstances. *See United States v. Lartey*, 716 F.2d 955, 961-62 (2d Cir. 1983); *Consumer Credit Ins. Agency, Inc. v. United States*, 599 F.2d 770, 777 n.1 (6th Cir. 1979), *cert. denied*, 445 U.S. 903 (1980); *In re Nwamu*, 421 F. Supp. 1361, 1365-67 (S.D.N.Y. 1976); *United States v. Re*, 313 F. Supp. 442, 448 (S.D.N.Y. 1970); U.S. Attorney's Manual, § 9-11.140 (forthwith subpoenas may be used "only when an immediate response is justified" and "only with the prior approval of the United States Attorney."). Even if there were sufficiently exigent circumstances, there is no longer a danger that evidence will be destroyed once the government has possession of the computer. Thus, the government must then obtain a warrant to search the contents. *See, e.g.*, *Horton*, 496 U.S. at 141 n.11; *David*, 756 F. Supp. at 1392.

If the government uses a forthwith subpoena to obtain possession of a portable computer because it is unsure of its location, this is not a valid use of a forthwith subpoena because it circumvents the requirement of probable cause to believe that evidence of a crime exists in a particular location. *See United States v. Nafzger*, 965 F.2d 213, 216 (7th Cir. 1992). The inconvenience of further investigation, or of obtaining a warrant in more than one district, should not excuse a failure to comply with the warrant requirement.[15] *Coolidge*, 403 U.S. at 481.

Before producing a computer or computer media pursuant to a subpoena, have a technical expert make a mirror image so that you will have an accurate copy of the information as it existed when your client last possessed it. This procedure will not leave a trace.

V. Some Common Government Defenses

A. Consent

A consensual search may not exceed the scope of the consent given, as determined by what a reasonable person would have understood by the exchange between the officer and the suspect. *See United States v. Turner*, 169 F.3d 84, 87 (1st Cir. 1999). Thus, for example, when the officers say they are looking for narcotics, physical evidence of an assault by an intruder, or a stolen television set, they may not use the suspect's consent as a license to search through the suspect's papers or computer files where the "expressed object" of the search is unlikely to be. *Id*. at 87-88. Furthermore, consent to seize a computer does not authorize the opening of files within the computer, *Carey*, 172 F.3d at 1274, nor does consent to "look at" a pager, computer or other electronic storage device authorize the activation of the device and search of its memory. *See United States v. Blas*, No. 90-CR-162, 1990 WL 265179, **19-21 (E.D. Wis. Dec. 4, 1990).

[15] With the USA Patriot Act, warrants for stored electronic communications covered by the Electronic Communications Privacy Act may be obtained from any federal court without geographic limitation, *see* 18 U.S.C. § 2711(3), and in an investigation of domestic or international terrorism, a warrant may be issued by a magistrate in any district in which activities related to the terrorism may have occurred for a search of property or for a person within or outside the district. *See* Fed. R. Crim. P. 41(a)(3).

A defendant may effectively limit consent to a search of particular files or areas within his computer. *See Commonwealth v. Hinds*, 437 Mass. 54, 59-60 & n.2 (2002).

Contrary to these authorities is a recent case from the Southern District of New York involving the investigation of a student from Quatar based on an apparently unfounded report that he was implicated in terrorism. There the court (not quite accurately) asserted that "[c]ourts have uniformly agreed that computers should be treated as if they were closed containers," *United States v. Al-Marri*, No. 02 Cr. 147(VM), 2002 WL 31519619, *6 (S.D.N.Y. Nov. 12, 2002), citing only *Runyan* (which took that view) and *Barth* (which viewed each computer *file* as a separate closed container). *See* Part III(B)(2), *supra*. By analogizing the computer to a closed container in an automobile and ignoring the law requiring a warrant to search the contents of a container in other contexts, *id*., the court went on to hold that separate consent to search the defendant's computer back at the FBI lab was not required once he consented to a search of his apartment. *Id*. The rule regarding closed containers in automobiles, however, originated in cases involving searches for discrete items like weapons or contraband in bags or suitcases that, along with the automobile, were mobile and therefore able to disappear. *See* Winick, 8 Harv. J.L. & Tech. at 82, 109-110. That rationale plainly does not apply to a computer containing a potentially large and diverse quantity of information in the possession of law enforcement agents who had plenty of time to get a warrant if they could come up with probable cause.

As to third party consent, a user of a shared computer has no authority to consent to a search of a co-user's password-protected files because such files are analogous to a locked footlocker in a shared home. *See Trulock v. Freeh*, 275 F.3d 391, 402-03 (4th Cir. 2001). And depending on the jurisdiction, the consent of a third party with no actual or apparent ownership interest in a computer may be invalid to support a seizure of the computer because the third party cannot permit others to take (as opposed to look at) something he himself has no right to take. *See People v. Blair*, 748 N.E.2d 318, 324-26 (Ill. App. Ct. 2001).

B. Good Faith

The good faith exception applies if the search was conducted in objectively reasonable reliance on a defective warrant. It does not apply if "a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984). The good faith of both the officers who execute the warrant and those who obtain it or provide information for it is at issue. *Id.* at 922-23 n.24. Accordingly, the case agent is not free to draft a warrant that fails to minimize intrusions on privacy and then defend the search based on the good faith of the computer specialist who executed it.

The good faith defense is not available at all if the police disregard a valid warrant. Thus, where agents did not rely on the precise language of a computer search warrant but instead developed a different search methodology and list of items to seize, the government's claim of good faith failed. *Maxwell*, 45 M.J. at 421.

The DOJ manuals, as well as training manuals for computer searches used by the FBI or other law enforcement agency involved, provide fruitful cross examination on how a well trained

officer would draft and execute a computer search warrant. The failure to keep careful and complete records is one of many issues relating to good faith likely to arise in any computer search. The DOJ, of which the FBI is a part, directs computer analysts to "document all the steps taken in the search," and keep "a careful record so that their efforts can be recreated for a court." *See Searching and Seizing Computers 1994*, Part IV(G)(3). Agency manuals contain similar and more stringent requirements. Because computer searches are usually conducted without witnesses, are complex and difficult to verify, and impossible to reconstruct from memory months or years later, a failure to keep careful records is objectively unreasonable.

It also is objectively unreasonable to fail to use the technical means available to narrow a computer search consistent with the needs of the case. As the *Gray* case, *see* Part III(B)(2), *supra*, and others[16] demonstrate, the Fourth Amendment can be eviscerated when courts fail to hold the government accountable to do so. Claims by government computer experts that they do not have the software or skill to perform a targeted search are not only objectively unreasonable, but may support an argument that their testimony should be excluded under Fed. R. Evid. 702. *See Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 153-54 (1999).

Government agents also must comply with the Stored Communications Privacy Act (SCA), 18 U.S.C. §§ 2701-11 in searching and seizing information in electronic storage, and with the Privacy Protection Act, 24 U.S.C. § 2000aa, in searching and seizing work product or other documentary materials intended for dissemination to the public. If a computer search is likely to reach any such materials, special provisions pertaining to these statutes must be made in the search warrant, and failure to comply with them can show bad faith. Under the SCA, the only remedy is civil, but the Fourth Amendment may provide a suppression remedy under certain circumstances.[17]

C. Plain View

To justify a seizure of evidence under the plain view exception, the government must prove that (1) the agent was lawfully at the place where the evidence could be plainly viewed, (2) it was "immediately apparent" that there was probable cause to believe that the evidence was evidence of a crime, and (3) the agent had a lawful right of access to the evidence itself. *See Horton v. California*, 496 U.S. 128, 136-37 (1990); *Searching and Seizing Computers 2001*, Part I(C)(3). In *Horton*, the Supreme Court eliminated the inadvertence requirement, but stressed that the particularity and probable cause requirements must be scrupulously adhered to in order to prevent the plain view doctrine from being misused to conduct general exploratory searches. *Horton*, 496 U.S. at 140 (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

---

[16] In *Commonwealth v. Ellis*, the Commonwealth's computer expert ran a keyword search using a certain program that would not allow him to retrieve the information on a physical level, then switched to a visual review of file names and file text, during the course of which he found and seized material of evidentiary value not described in the warrant. *Id*. at *4. He claimed he tried but failed to find a program to retrieve information on a physical level. *Id*. Though he later did find one, *id*. at 6, the court ruled that the material he seized while performing his visual review was legitimately in plan view. *Id.* at *12-13.

[17] *See Maxwell*, *supra*, 45 M.J. at 417-19. For a discussion of the issue of whether and when the Fourth Amendment may protect electronic mail, *see* Amicus Curiae Brief of Professor Orin S. Kerr in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002). In *Bach*, the Eighth Circuit noted but did not reach the question.

The plain view exception does not justify a search of the contents of a closed file folder or notebook that lacks external indicia of probable cause. *Knoll*, 16 F.3d at 1321; *United States v. Whitten*, 706 F.2d 1000, 1013 (9th Cir. 1983). Likewise, if in a computer search the agent has to open or otherwise manipulate a file or area of the computer not described in the warrant in order to view its contents and see indicia of probable cause, the contents were not in plain view. *See Carey*, 172 F.3d at 1273; *Maxwell*, 45 M.J. at 422; *Smith v. State*, 713 N.E.2d 338, 345 (Ind. Ct. App. 1999); *Searching and Seizing Computers 2001*, Part I(C)(3); *cf. Hicks*, 480 U.S. at 324-35 (serial numbers were not in plain view where agent had to move stereo equipment in order to see them). Thus, once the agent sees something whose incriminating nature is immediately apparent in plain view and confirms it by viewing that file, he must obtain a second warrant before searching for any additional evidence of the same character. *Carey*, 172 F.3d at 1272-73.

Challenging an agent's assertion that he was lawfully in an area of the hard drive from which he viewed the evidence is often more difficult than in a physical search. In the search of a house, an agent cannot rely on the plain view exception if in looking for a gun he opened a tiny jewelry box and found cocaine, since it is obvious that he had no authority to look in the jewelry box because of its physical size. In a computer search, whether the agent was in a lawful position to view and access the evidence will depend on the attributes and nature of the file or space in which the evidence is viewed, whether the warrant authorized a search of that file or space, and whether the government used appropriate technical means to get there. For example, the exception fails if the warrant is for documents containing certain keywords and the file (or area of free or slack space) claimed to have been in plain view did not contain any of those keywords.

VI. Discovery and Pre-Suppression Motions

You will need every bit of contemporaneous evidence of the search in order to reconstruct and test the government's search. If it does not exist, ask the court to draw an adverse inference.

As noted above, there should be a written record of the search, as well as audit logs and time stamps that are automatically generated in the course of the search. The government may claim that the latter are sufficient and that no written records exist or were required to be kept. This is wrong. *Searching and Seizing Computers 1994*, Part IV(G)(3).

You should also move for the physical evidence. This will consist of both a copy of the pristine mirror image, and the "working copy," which is the mirror image restored to a clean hard drive and then searched. *See Searching and Seizing Computers 2001*, Part II(B)(1) n.5. If the computer has been seized from the premises, you can file a motion asking the magistrate to require the return of the computer, leaving the prosecution with an imaged copy of the hard drive. *See* Fed. R. Crim. P. 41(e); *Searching and Seizing Computers 2001*, Parts I(B)(1), II(C)(Step 3) & App. F, Part II(C); *Commonwealth v. Sacco*, 401 Mass. 204, 206 (1987). Alternatively, the court should require that a mirror image be given to you. *See Ellis*, supra.

The working copy is your crime scene because it can indicate which files were searched and when by showing more recent access dates than those on a hard drive or image that has not been searched. If the government restores and searches the image several times, more than one working copy will be created, but each one may be wiped clean before restoring and searching the next one. Because government computer analysts regularly wipe and reuse working copies (claiming lack of resources to purchase more $69 hard drives), write to the prosecutor and file a motion with the judge requesting that each one be preserved as soon as you are aware of the search.

In any case where child pornography is allegedly on the computer, the prosecution may take the position that giving copies to the defense constitutes unlawful dissemination of child pornography and thus, you may not have a copy, and at best, may review it on their premises and under their supervision. The California Court of Appeal ruled in such a case that construing the statute in that manner "exalts absurdity over common sense," and that requiring the defense to view the data at the FBI's offices "obviously impacts [the defendant's] right to effective assistance of counsel." Westerfield v. Superior Court, 121 Cal. Rptr.2d 402 (2002). Instead, the court could issue a protective order limiting disclosure to counsel and their agents and/or order the copies returned at the conclusion of the case. Id.

Another type of physical evidence is an audit log. The program used to make and restore images should have an audit function that shows every operator entry and its date and time, and also errors encountered in the process. As a result, the audit log can tell you how many mirror images were made and when, and how many were restored to a hard drive and when. The audit function is a default feature that runs automatically on most forensic imaging software including SafeBack and EnCase which the FBI generally uses. If the audit log does not exist, the agent must have intentionally rejected it.

As noted in Part III(B)(1)(b), *supra*, the government's computer analyst may save all or some of the active files, deleted files, slack space, and/or free space from a working copy to CDs (which are read-only) or magneto optical disks (which can be write-protected) so that the case agent can search them, perhaps without regard for time or probable cause-based limits, without leaving a trace. This is not necessary to preserve the original evidence and not a technically necessary part of the search itself. The original image serves to permanently preserve the evidence. Once the image is restored to a working copy, the working copy can be directly searched for evidence using a wide variety of commonly available software tools, such as EnCase and FTK, without the risk of altering the data under search. Using such tools provides the added benefit of creating and maintaining an automated log, which provides a complete record of every action performed during the search. Thus, copying to CDs or magneto optical disks serves no legitimate purpose and may be used to obscure an overbroad search. As soon as you are aware of the search, you should move that this procedure not be used because it will prevent there being a physical record of what files and data were opened and viewed. If your motion is denied or too late, you should argue that this was a seizure beyond the scope of the warrant, and that you are entitled to these media as part of the inventory of items seized.

Finally, you should obtain copies of the exact same programs the government used. *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir.), *cert. denied*, 400 U.S. 825 (1970). If

they are a type that is available only to law enforcement, a protective order may be necessary, and your expert may even have to use the program in a law enforcement facility.